#3

Atty. Dkt. No. 068398-0104

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Virgil D. Gligor et al.
Title:	AUTHENTICATION METHOD AND SCHEMES FOR DATA INTEGRITY PROTECTION
Appl. No.:	09/818,608
Filing Date:	March 28, 2001
Examiner:	Unassigned
Art Unit:	2131

SUBSTITUTE INFORMATION DISCLOSURE STATEMENT UNDER 37 CFR §1.56

Commissioner for Patents
Washington, D.C. 20231

Sir:

Submitted herewith is a substitute information disclosure statement in connection with the above identified application. This substitute information disclosure statement is being filed to replace the information disclosure statement filed on June 28, 2001 as there were missing pages in some of the references filed. Also, additional references are included in this information disclosure statement.

The submission of any document herewith, which is not a statutory bar, is not intended as an admission that such document constitutes prior art against the claims of the present application or that such document is considered material to patentability as defined in 37 CFR §1.56(b). Applicants do not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference any document which is determined to be a *prima facie* art reference against the claims of the present application.

Atty. Dkt. No. 068398-0104

TIMING OF THE DISCLOSURE

The listed documents are being submitted in compliance with 37 CFR §1.97(b), before the mailing date of the first Office Action on the merits.

Applicants respectfully request that any listed document be considered by the Examiner and be made of record in the present application and that an initialed copy of Form PTO-1449 be returned in accordance with MPEP §609.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

Respectfully submitted,

Date July 24, 2001

By ____________________

William T. Ellis
Attorney for Applicant
Registration No. 26,874

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

Page 1 of 1

Form PTO-1449 (MODIFIED)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. 068398-0104	SERIAL NO. 09/818,608
		APPLICANT Virgil D. Gligor et al.	
INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*		FILING DATE March 28, 2001	GROUP ART UNIT 2131

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
	A1	5,757,913	5/26/98	Bellare et al.	380	23	

FOREIGN PATENT DOCUMENTS

	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION	
							YES	NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

	A2	Virgil D. Gligor et al., "Object Migration and Authentication.", IEEE Transactions on software Engineering, vol. SE-5, No. 6, November 1979, pp. 607-611
	A3	Alfred J. MENEZES et al., ""Handbook of Applied Cryptography", pp. 321-367, (1965)
	A4	J. Black et al., "UMAC: Fast and Secure Message Authentication.", Advances in Cryptology-CRYPTO '99, pp. 216-233
	A5	Mihir BELLARE et al., "Keying Hash Functions For Message Authentication", Springer-Verlag Berlin Heidelberg, pp. 216-233, (1996)
	A6	Mihir BELLARE et al., "The Security of Cipher Block Chaining.", Advances in Cryptology-CRYPTO '94, pp. 341-358
	A7	Federal Information Processing Standards Publication 46-1, Data Encryption Standard (DES), pp. 1-16, (1988)
	A8	Federal Information Processing Standards Publication 46-2, Data Encryption Standard (DES), pp. 1-18, (1993)
	A9	Erez PETRANK et al., "CBC MAC For Real-Time Data Sources", Federal Information Processing Standards Publication 46-2, Data Encryption, pp. 1-23, (1993)
	A10	American National Standard ANSI X9.9 (1986) pp. 6-8
	A11	Mihir BELLARE et al., "XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions", pp. 1-20, (1995) Preliminary version appearing in Advances in Cryptology-CRYPTO '95, Lecture Notes in Computer Science vol. 963.
	A12	Mihir BELLARE et al., "Incremental Cryptography and Application to Virus Protection.", pp. 1-15, (1995), Abstract appearing in Proceedings of the 27th ACM Symposium on the Theory of Computing, May (1995)
	A13	Moni NAOR et al., "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs.", Advances In Cryptology-CRYPTO '98, Springer-Verlag Berlin Heidelberg, pp. 265-282, (1998)
	A14	Mihir BELLARE et al., "A Concrete Security Treatment of Symmetric Encryption", Proceedings of the 38th Sympposium on Foundations of Computer Science, IEEE,(1997) pp. 394-403
	A15	Donald E. KNUTH., "The Art of Computer Programming-Vol. 2: Seminumerical Algorighms.", Addison-Wesley, (1981) (Second Edition), Chapter 3.

EXAMINER	**DATE CONSIDERED**

* **EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.**